

05-11-2004

2002P0350
PCT/DE03/0302910/533083 DE0303029
JC12 Rec'd PCT/PTC 28 APR 2005

7

gesamten Datenverkehrs ausgebildet und auch auf die spezifischen Übertragungsprotokolle aller in Frage kommenden Anwendungen eingerichtet sein muss.

5

Ein weiterer Nachteil ist derjenige, dass bei Datenpaketen, die aus dem Internet bei der NAT-Instanz ankommen und keine Antwort auf eine bereits zuvor von einem Netzelement des lokalen Netzwerks versendeten Datenpaket darstellen, in der 10 NAT-Instanz keine gespeicherten Informationen über den "richtigen" Empfänger vom lokalen Netzwerk vorliegen.

Dieser Nachteil wird teilweise dadurch umgangen, dass für 15 eine Reihe bekannter IP-Port-Nummern für ankommende und nicht anhand gespeicherter Informationen zuzuordnenden Datenpaketen ein Ziel-Netzelement vordefiniert wird. Man spricht in diesem Zusammenhang auch von "Exposed Machines". Man macht sich dabei zu nutze, dass eine Reihe von IP-Port-Nummern, man spricht auch von Well-Known-Ports, jeweils einem bestimmten 20 Anwendungstyp zugeordnet sind und somit von der NAT-Instanz an ein (bzw. das) Netzelement mit der entsprechenden Anwendung adressiert werden können. Diese Form des Routings ist allerdings für jede IP-Port-Nummer auf eine einzige Anwendung und damit auf ein einziges Netzelement des lokalen 25 Netzwerks beschränkt.

Die Druckschrift WO 01/71977 A2 Bosco et al. „Home- 30 Networking“ zeigt eine Anordnung, in der mehrere Netzelemente („client device“) über eine Netzknoteneinrichtung („home gateway device“) mit einer externen Einrichtung („Host System“) verbunden sind. Die Netzknoteneinrichtung umfasst dabei eine Adressumsetzungseinrichtung (NAT-Instanz), wodurch die lokalen Adressen der Netzelemente in eine globale Adresse der externen Einrichtung umgesetzt wird, und umgekehrt. Für 35 Anwendungen, bei denen einem der Netzelemente eine globale Adresse durch die externe Einrichtung zugewiesen werden soll, baut die Netzknoteneinrichtung nach Anforderung

7a

durch die Anwendung eine Tunnelverbindung stellvertretend für das betroffene Netzelement zu der externen Einrichtung auf, wobei der betroffenen Anwendung die netzwerkseitige globale

5 IP-Adresse der Tunnelverbindung zugeordnet wird und wobei die für die Anwendung bestimmten getunnelten Daten der Anwendung von der Netzknotteneinrichtung übermittelt werden

In vielen Fällen ist der sicherste und in der Praxis einzige
10 gangbare Weg zur Nutzung bestimmter Anwendungen derjenige, dass das entsprechende Netzelement einer solchen Anwendung direkt, also unter Ausschluss des Routers, mit dem Modem verbunden wird. Dann erfolgt der PPTP-Tunnelaufbau nicht mehr zwischen einer logischen Instanz des Routers und dem Modem,
15 sondern zwischen dem betroffenen Netzelement selbst und dem Modem. Damit wird die PPP-Verbindung direkt zwischen dem Netzelement und dem Internet-Dienste-Anbieter aufgebaut. Dem Vorteil, dass dem Netzelement selbst somit die global eindeutige Internetadresse zugewiesen wird und somit auch die
20 beschriebenen Anwendungen mit den besonderen Anforderungen

BEST AVAILABLE COPY

GEÄNDERTES BLATT

05-11-2004

2002P03503 WO

PCT/DE03/03029

DE0303029

17

Patentansprüche

1. Verfahren zum Austausch von Daten zwischen einer externen Einrichtung (ISP) und auf Netzelementen (PC) eines paketvermittelnden Netzwerks installierten Anwendungen mittels zumindest einer Tunnelverbindung,
 - bei dem jedes Netzelement (PC) an einer Netzknoteneinrichtung (ROU) angeschlossen ist,
 - bei dem die Netzknoteneinrichtung (ROU) an der Tunnelverbindung beteiligt ist und
 - bei dem dem netzwerkseitigen Endpunkt der getunnelten Verbindung eine globale Adresse eindeutig zugeordnet wird, wobei bei mehreren die Tunnelverbindung gemeinsam nutzenden Netzelementen (PC) die Netzknoteneinrichtung (ROU) den netzwerkseitigen Endpunkt der Tunnelverbindung bildet, dadurch gekennzeichnet, dass eines der Netzelemente (PC), wenn es für die Ausführung einer Anwendung eine globale Adresse benötigt, eine Tunnelverbindung aufbaut und deren netzwerkseitigen Endpunkt bildet, wobei diese Tunnelverbindung nur von diesem Netzelement (PC) genutzt wird und wobei alle Daten durch die Netzknoteneinrichtung (ROU) geleitet werden, und dass die Netzknoteneinrichtung (ROU) wechselweise oder gleichzeitig Endpunkt oder datendurchleitende Instanz einer Tunnelverbindung und/oder mehrerer Tunnelverbindungen sein kann.
2. Verfahren nach einem der vorhergehenden Ansprüchen, dadurch gekennzeichnet, dass die Tunnelverbindung eine nach dem PPTP-Tunneling-Protocol arbeitenden Verbindung ist, die die Daten einer getunnelten Verbindung unbeeinflusst überträgt.

BEST AVAILABLE COPY

GEÄNDERTES BLATT

05-11-2004

200203505

DE0303029

18

3. Verfahren nach einem der vorhergehenden Ansprüchen, dadurch gekennzeichnet, dass die Netzelemente (PC) PCs sind und die externe Einrichtung (ISP) ein über ein DSL-Modem (MODEM) angeschalteter Internet-Dienste-Anbieter ist.
4. Verfahren nach einem der vorhergehenden Ansprüchen, dadurch gekennzeichnet, dass den Netzelementen (PC) lokale, nur in dem paketvermittelnden Netzwerk (LAN) eindeutige Adressen zugewiesen sind.
5. Verfahren nach einem der vorhergehenden Ansprüchen, dadurch gekennzeichnet, dass die Netzknotteneinrichtung (ROU) ein Router ist, der eine Instanz zum Aufbau und Betrieb einer PPTP-Tunnelverbindung aufweist.

BEST AVAILABLE COPY**GEAENDERTES BLATT**

05-11-2004

200203505

DE0303029

19

6. Netzknoteneinrichtung, die am Austausch von Daten mittels zumindest einer Tunnelverbindung zwischen einer externen Einrichtung (ISP) und auf Netzelementen (PC) eines paketvermittelnden Netzwerks installierten Anwendungen 5 beteiligt ist,

- bei dem jedes Netzelement (PC) an einer Netzknoteneinrichtung (ROU) angeschlossen ist und
- bei dem dem netzwerkseitigen Endpunkt der getunnelten Verbindung eine globale Adresse eindeutig zugeordnet ist,

10 wobei bei mehreren die Tunnelverbindung gemeinsam nutzenden Netzelementen (PC) die Netzknoteneinrichtung (ROU) den netzwerkseitigen Endpunkt der Tunnelverbindung bildet, dadurch gekennzeichnet, dass durch eines der Netzelemente (PC), wenn es für die 15 Ausführung einer Anwendung eine globale Adresse benötigt, eine Tunnelverbindung aufbaubar ist und dann deren netzwerkseitigen Endpunkt bildet, wobei diese Tunnelverbindung nur von diesem Netzelement (PC) nutzbar ist und wobei eine Durchleitung aller Daten durch die 20 Netzknoteneinrichtung (ROU) erfolgt.

BEST AVAILABLE COPY**GEAENDERTES BLATT**

analyze the entire data traffic and also needs to be set up for the specific transmission protocols of all possible applications.

- 5 A further drawback is that in the case of data packets which arrive at the NAT entity from the Internet and are not a response to a data packet which has already been sent by a network element of the local area network previously, the NAT entity does not contain any
- 10 stored information about the "correct" receiver from the local area network.

This drawback is partially overcome by virtue of a destination network element being predefined for a

- 15 series of known IP port numbers for incoming data packets which cannot be allocated using stored information. In this context, reference is also made to "exposed machines". Here, use is made of the fact that a series of IP port numbers (also referred to as well-
- 20 known ports) each have a particular associated application type and can thus be sent from the NAT entity to a (or the) network element with the appropriate application. This form of routing is limited to a single application for each IP port number
- 25 and thus to a single network element of the local area network, however.

The document WO 01/71977 A2 Bosco et al. "Home Networking" shows an arrangement in which a plurality of network elements ("client device") are connected to an external device ("host system") via a network node device ("home gateway device"). In this arrangement, the network node device comprises an address conversion device (NAT entity), which converts the local addresses of the network elements into a global address for the

- 7a -

external device, and vice versa. For applications in which one of the network elements is intended to be allocated a global address by the external device, the network node device sets up a tunnel connection which

5 is representative of the network element in question to the external device upon request by the application, the application in question being assigned the network's global IP address of the tunnel connection, and the tunneled data intended for the application

10 being transmitted to the application by the network node device.

In many cases, the safest and in practice only feasible way of using particular applications is for the

15 appropriate network element of such an application to be connected to the modem directly, that is to say with the exclusion of the router. In that case, the PPTP tunnel setup is no longer effected between a logical entity of the router and the modem, but rather between

20 the affected network element itself and the modem. The PPP connection is thus set up directly between the network element and the Internet service provider. The advantage that the network element itself is thus allocated the globally unique Internet address and

25 hence also that the applications described can be operated with

Patent Claims

1. A method for interchanging data between an external device (ISP) and applications installed on network elements (PC) of a packet-switching network using at least one tunnel connection,
 - in which each network element (PC) is connected to a network node device (ROU),
 - in which the network node device (ROU) is involved in the tunnel connection, and
 - in which the network-end terminal point of the tunneled connection is allocated a global address uniquely, with the network node device (ROU) forming the network-end terminal point of the tunnel connection when there are a plurality of network elements (PC) with joint use of the tunnel connection, characterized in that if one of the network elements (PC) requires a global address for executing an application it sets up a tunnel connection and forms the latter's network-end terminal point, this tunnel connection being used only by this network element (PC), and all data being routed through the network node device (ROU), and
 - 25 in that the network node device (ROU) may alternately or simultaneously be a terminal point or a data-routing entity of a tunnel connection and/or of a plurality of tunnel connections.
- 30 2. The method as claimed in one of the preceding claims, characterized in that the tunnel connection is a connection which operates on the basis of the PPTP tunneling protocol and which transmits the data in a tunneled connection without influence.

3. The method as claimed in one of the preceding claims,
characterized
in that the network elements (PC) are PCs and the
5 external device (ISP) is an Internet service provider
connected by means of a DSL modem (MODEM).

4. The method as claimed in one of the preceding
claims,
10 characterized
in that the network elements (PC) have associated local
addresses which are unique only in the packet-switching
network (LAN).

15 5. The method as claimed in one of the preceding
claims,
characterized
in that the network node device (ROU) is a router which
has an entity for setting up and operating a PPTP
20 tunnel connection.

6. A network node device which is involved in the interchange of data using at least one tunnel connection between an external device (ISP) and applications installed on network elements (PC) of a
5 packet-switching network,

- in which each network element (PC) is connected to a network node device (ROU), and
- in which the network-end terminal point of the tunneled connection has a uniquely allocated
10 global address,

with the network node device (ROU) forming the network-end terminal point of the tunnel connection when there are a plurality of network elements (PC) with joint use of the tunnel connection,

15 characterized

in that if one of the network elements (PC) requires a global address for executing an application it can set up a tunnel connection and then forms the latter's network-end terminal point, this tunnel connection
20 being able to be used only by this network element (PC), and all data being routed through the network node device (ROU).